Innominate mGuard

Frequently Asked Questions (FAQ)

mGuard smart   **mGuard centerport**   **mGuard blade**

mGuard industrial RS   **mGuard PCI**   **mGuard delta**

Table of Contents

1   Disclaimer

© Innominate Security Technologies AG

October 2009
"Innominate" and "mGuard" are registered trademarks of the Innominate Security Technologies
AG. All other brand names or product names are trade names, service marks, trademarks, or
registered trade marks of their respective owners.
mGuard technology is protected by the German patents #10138865 and #10305413. Further
national and international patent applications are pending.
No part of this documentation may be reproduced or transmitted in any form, by any means
without prior written permission of the publisher.
All information contained in this documentation is subject to change without previous notice.
Innominate offers no warranty for these documents. This also applies without limitation for the
implicit assurance of scalability and suitability for specific purposes.
In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental
or otherwise, caused in connection with delivery, output or use of these documents.
This documentation may not be photocopied, duplicated or translated into another language, either
in part or in whole, without the previous written permission of Innominate Security Technologies
AG.

2   Configuration

2.1   General Questions

2.1.1   Do I need to install a driver for the mGuard?

The installation of a driver is only required when using the mGuard PCI in *Driver* mode. In this case a driver for the PCI interface of the mGuard PCI (available for Windows XP/2000 and Linux) needs to be installed on the computer which will provide a "regular" network interface with additional security functions. All other products will be configured completely through their web interface.

2.1.2   I need help in configuring the mGuard (Router, PPPoE, VPN, L2TP)

Please download the document *mGuard Configuration Examples* from our homepage (www.innominate.com -> *Downloads -> Documentation*). This document explains in detail on a basis of several examples how to configure the mGuard for the different operating modes (Router, PPPoE, Stealth) and scenarios (VPN, L2TP/IPsec, firewall redundancy, router redundancy, 1:1 NAT, etc.).

2.1.3 In which case do I need to use which network mode (Stealth, Router, PPPoE/PPTP, Modem/Modem-internal)?

Stealth mode:
If the mGuard is operated in *Stealth* mode you don't need to reconfigure the clients which are connected to the internal interface of the mGuard. You simply need to interconnect the mGuard between the clients which need to be protected and the network. The IP addresses of the clients do not change. All processes, which are listening on a port, are hidden to the network and won't be detected by a port scanner. The mGuard works completely transparent.

Stealth - autodetect and static:
The *Stealth* modes *autodetect* or *static* can by used if the mGuard should protect one single entity (e.g. server) and if the NIC of the client has only one IP address. Otherwise the *multiple clients Stealth* mode needs to be used.

When using *autodetect Stealth* mode, the mGuard detects its IP address automatically by analyzing the traffic which comes from the internal network and adopts the IP and MAC address of the client. Some entities do not generate traffic by itself (e.g. server, webcam) so the mGuard will never get its IP settings. In this case you need to use *static Stealth* mode and specify at least the clients IP address in the menu *Network -> Interfaces*, tab *General*.

The web interface of the mGuard can be accessed from the internal network through the URL https://1.1.1.1 and from the external network by using https://<IP address of the client> assuming that HTTPS remote access is enabled (menu *Management -> Web Settings*, tab *Access*).

Stealth - multiple clients:
This mode is used if the mGuard should protect multiple clients or if the NIC of a single client has more than one IP address.

The web interface of the mGuard can be accessed from the internal network by using the URL https://1.1.1.1 as long as no *Management IP* was specified. If the web interface should be accessible from the external network, enable HTTPS remote access (menu *Management -> Web Settings*, tab *Access*) and specify a *Management IP* in the menu *Network -> Interfaces*, tab *General*. Now you can access the mGuard through the URL https://<Management IP> from the internal and external network.

Router mode:
In *Router* mode the mGuard acts as a router between two different networks. You need to configure the internal and external interface.

The web interface of the mGuard can be accessed from the internal network through the URL https://<internal IP of the mGuard> and from the external network by using https://<external IP of the mGuard> (assuming that HTTPS remote access is enabled, menu *Management -> Web Settings*, tab *Access*).

PPPoE/PPTP mode:
In *PPPoE* mode the mGuard acts as a DSL router between the internal network and the Internet. The external interface of the mGuard needs to be connected to a DSL modem. You need to configure the internal interface. The mGuard will receive its external IP settings from the Internet Service Provider (ISP). *PPTP* is the equivalent to *PPPoE*, and is used for example in Austria.

The web interface of the mGuard can be accessed from the internal network through the URL https://<internal IP of the mGuard> and from the external network by using https://<external IP of the mGuard> (assuming that HTTPS remote access is enabled, menu *Management -> Web Settings*, tab *Access*).

Modem/Modem-internal:

This network mode is used if the mGuard is located in a network which does not have access to the Internet and:

- if you need remote access to the mGuard or
- if you need remote access to the machines which are connected to the internal interface of the mGuard or
- if the mGuard should establish a VPN connection through a phone line to a remote VPN gateway.

All traffic directed to the external interface (WAN port) will be redirected through the serial port of the mGuard to a modem. You can either connect an external modem to the serial port of the mGuard (network mode **Modem**) or use the internal modem (analog modem/ISDN TA adapter) of the mGuard industrial RS (network mode **Modem-internal**) if available.

2.1.4   mGuard smart: the middle LED flashes red continuously. What happened?

If the middle LED flashes red continuously then the mGuard couldn't start because some files used by the kernel are missing. This could happen if a flash procedure was interrupted. Flash the mGuard with the current firmware version. This should solve the problem.

2.1.5   Is it possible to change the MTU size?

It is possible to change the MTU sizes for the internal and external Ethernet interfaces through the menu *Network -> Interfaces*, tab *Ethernet*.

2.1.6   Do I need to use a cross link cable?

Not necessarily. The mGuard detects automatically the type of the connected cable and the transfer rate.

2.1.7   May I connect ISDN directly to the mGuard (LAN/WAN port)?

NO! The connectors of the mGuard are for Ethernet connections only. You may use an ISDN router, which provides an Ethernet interface. Connecting the mGuard to another device than an Ethernet connection may cause serious damage to the mGuard.
If you have an mGuard industrial RS with integrated ISDN TA adapter the lower terminal block provides the required connector pins.

2.1.8   Is it possible to specify a NBNS (WINS) server apart from the DNS server?

A WINS server can be specified through the menu *Network -> DHCP*, tabs *Internal/External DHCP*.

2.1.9   What is Network Address Translation (NAT)?

NAT (Network Address Translation) is the translation of an internet protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also reduces the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.
If the mGuard is used as gateway to the Internet, NAT must be activated.

2.1.10 What is Network Address Translation Traversal (NAT-T)?

The problem with NAT and IPSec (VPN connections)
Why doesn't NAT work with IPSec? Remember that the point of IPSec is not just to protect the confidentiality of the data, but also to assure the authenticity of the sender and the integrity of the data (that it hasn't been changed in transit). The problem with NAT is obvious: NAT must change information in the packet headers in order to do its job.

The first problem is that NAT changes the IP address of the internal computer to that of the NAT device. The Internet Key Exchange (IKE) protocol used by IPSec embeds the sending computer's IP address in its payload, and this embedded address doesn't match the source address of the IKE packet (which is that of the NAT device). When these addresses don't match, the receiving computer will drop the packet.

Another problem is that TCP checksums (and optionally, UDP checksums) are used to verify the packets. The checksum is in the TCP header and it contains the IP addresses of the sending and receiving computers and the port numbers used for the communications. With normal NAT communications, this isn't a problem because the NAT device updates the headers to show its own IP address and port in place of the sending computers. However, IPSec encrypts the headers with the Encapsulating Security Payload (ESP) protocol. Since the header is encrypted, NAT can't change it. This means the checksum is invalid, so the receiving computer rejects the packet.

In addition, NAT isn't able to use the port numbers in TCP and UDP headers to multiplex packets to multiple internal computers when those headers have been encrypted by ESP.

NAT-T: How it works
The IPSec working group of the IEEE has created standards for NAT-T that are defined in RFCs 3947 and 3948. NAT-T is designed to solve the problems inherent in using IPSec with NAT.

NAT-T adds a UDP header that encapsulates the ESP header (it sits between the ESP header and the outer IP header). This gives the NAT device a UDP header containing UDP ports that can be used for multiplexing IPSec data streams. NAT-T also puts the sending computer's original IP address into a NAT-OA (Original Address) payload. This gives the receiving computer access to that information so that the source and destination IP addresses and ports can be checked and the checksum validated. This also solves the problem of the embedded source IP address not matching the source address on the packet.

2.1.11 I have enabled remote access for HTTPS/SSH but it still doesn't work

Verify that you also have specified firewall rules (*Allowed Networks*) for the remote access (HTTPS: menu *Management -> Web Settings*, tab *Access*, SSH: menu: *Management -> System Settings*, tab *Shell Access*).

2.1.12 Do I need to enable remote access for configuring the mGuard from the client?

No, usually the clients connected to the internal interface of the mGuard have access to the device through SSH/HTTPS.

It is possible to block SSH and/or HTTPS access from the internal network (HTTPS: menu *Management -> Web Settings*, tab *Access*, SSH: menu: *Management -> System Settings*, tab *Shell Access*). If you disable SSH and/or HTTPS access from the internal network, ensure that you have enabled it for the external network first. Otherwise you won't have the possibility to gain access to the mGuard, neither through SSH nor through HTTPS, neither from the internal nor from the external network. In such a case you need to execute the *Recovery* procedure (refer to the *mGuard User Manual*). The *Recovery* procedure will remove defined SSH access rules and add a HTTPS access rule for allowing access from the internal network.

2.2   Stealth mode

2.2.1   What does Stealth mode mean?

If the mGuard is operated in *Stealth* mode you don't need to reconfigure the clients which are connected to the internal interface of the mGuard. You simply need to interconnect the mGuard between the clients which need to be protected and the network. The IP addresses of the clients do not change. All processes, which are listening on a port, are hidden to the network and won't be detected by a port scanner. The mGuard works completely transparent. You can't use the *Stealth* mode if the mGuard is connected to a DSL line. In this case you need to use the *PPPoE* or *PPTP* mode respectively combined with *Network Address Translation* (NAT).

2.2.2   Why must a desktop firewall on the client allow ICMP echo requests

The mGuard can't initiate ARP requests if it is operated in *Stealth* mode because it will never know if the response is related to an ARP request it has issued. For sending data to an external network (as it is the case e.g. for establishing a VPN connection or for the online update) the mGuard needs to know the MAC address of the default gateway. For obtaining it, the Guard sends a marked ICMP echo request to the client first by using the IP address of the destination as source IP address. When receiving the reply from the client, the mGuard filters out the MAC address of the default gateway.

2.2.3   What is the difference between the Stealth modes autodetect, static and multiple clients?

Please refer to In which case do I need to use which network mode (Stealth, Router, PPPoE/PPTP, Modem/Modem-internal)?.

2.2.4   It is not possible to "ping" the internal client of the mGuard

*   Verify that you have specified incoming firewall rules (menu *Network Security -> Packet Filter*, tab *Incoming Rules*) with Protocol=All or Protocol=ICMP. If this isn't the case the firewall will block the ICMP requests.
*   Check if there is a desktop firewall (e.g. WinXP SP2 firewall) running on the client, which blocks the ICMP requests.
*   Check if there is a software VPN client running on the client. Some VPN clients come with an integrated firewall (e.g. Cisco VPN Client, Checkpoint VPN Client) which blocks the ICMP requests.

2.2.5   I can't access the mGuard through https://1.1.1.1

*   At first verify that the web browser does not use a proxy (Internet Explorer: *Tools -> Internet Options*, tab *Connections*, button *<LAN Settings>*, section *Proxy server*). In this case the web browser would send the requests directly to the proxy.
*   Check if a desktop firewall is running on the client which prevents the access to the mGuard. If this is the case, disable the firewall and restart the computer.
*   Check with the command *ipconfig /all* if the Ethernet card has more than one IP address. We encountered this problem with an USB software (IP=192.168.100.100) which had sent the data through the wrong interface. In this case the mGuard would reconfigure itself every second for using the other IP address. You need to disable the software which assigned the second IP address to the computer in such a case.
*   A default gateway must be defined on the client. The mGuard captures all data traffic directed to the address 1.1.1.1 and uses it internally. If no default gateway is defined, the client will send data only to IP addresses, which belong to its own network (e.g. 192.168.1.0/24). In this case data directed to 1.1.1.1 will never reach the mGuard.

You need to consider the following points if the external interface of the mGuard is not connected to the network or if the specified default gateway on the client is not reachable:
*   Assign static IP settings to the client if the client is configured to receive the setting from a DHCP server (e.g. IP address = 192.168.1.100, subnet mask = 255.255.255.0, default gateway = 192.168.1.1). You must specify a default gateway even if the external interface of the mGuard is not connected to a network.
*   Assign a static MAC address to the IP address of the default gateway. The computer would try to retrieve the MAC address of the default gateway by sending an ARP request first. This of

course will fail because the default gateway is not reachable. For avoiding this, you need to assign an arbitrary static MAC address to the IP address of the default gateway with the ARP command (e.g. arp -s <IP of the default gateway> 00-aa-aa-aa-aa-aa). This way the client is happy because it already knows the MAC address of the default gateway and will send the data to the network. The mGuard will capture all packets directed to the address 1.1.1.1.

2.2.6   Does my computer need to belong to the same net as the mGuard (IP=1.1.1.1)?

No, definitely not. The address 1.1.1.1 is a pseudo address. All packets directed to this address will be captured by the mGuard and used internally. If you'd select an IP address and a netmask which belongs to the same net as the IP 1.1.1.1 (e.g. 1.1.1.2/255.255.255.0) then the IP 1.1.1.1 must be reachable directly by the computer. Your computer will send an ARP request to verify this. You won't get a connection to the mGuard because the mGuard in *Stealth* mode doesn't reply to ARP requests.

2.2.7   Why do I need to specify a default gateway?

The mGuard captures all packets directed to the address 1.1.1.1 and uses them internally. Therefore the packets must reach the mGuard. If you don't specify a default gateway, the client will send packets only to IP addresses which belong to its own network (e.g. 192.168.1.0/24). If the external interface of the mGuard is not connected to the network, you need to assign a static MAC address to the IP address of the default gateway. The computer would try to retrieve the MAC address of the default gateway by sending an ARP request first. This of course will fail because the default gateway doesn't really exist. For avoiding this, you need to assign an arbitrary static MAC address to the IP address of the default gateway with the ARP command (e.g. arp -s <IP of the default gateway> 00-aa-aa-aa-aa-aa). This way the client is happy because it already knows the MAC address of the default gateway and will send the data to the network. The mGuard will capture all packets directed to the address 1.1.1.1.

2.2.8   Web browser error message "Unknown host 1.1.1.1"

This error message appears when the web browser uses a proxy. In this case the data packets will be sent directly to the proxy and not to the IP address 1.1.1.1. Configure the web browser not to use a proxy.

2.2.9   Sometimes no access to the mGuard and interrupted connection to the network

Check with the command *ipconfig /all* if the NIC of the client has more than one IP address. If this is the case the mGuard (*Stealth autodetect* mode only) will reconfigure itself every second by adopting the senders IP address. This would make it almost impossible to gain access to the mGuard and the connection to the network will be interrupted. Use *Stealth multiple clients* mode for solving the problem.

2.2.10 Can I configure the mGuard remotely? Which IP do I have to use?

At first you need to enable remote access for SSH (menu: *Management -> System Settings*, tab *Shell Access*) and/or HTTPS (menu *Management -> Web Settings*, tab *Access*) and set the corresponding firewall rules (section *Allowed Networks*). For gaining remote access to the mGuard you need to specify the IP address of the client to which the mGuard is connected.

2.2.11 Windows Vista: "arp –s" doesn't work (Error code: 5)

With Windows Vista it is not possible to assign a static MAC address to the IP address of the default gateway using the arp program. You must use *netsh* from a command shell with administrator rights instead.

At first you need to know the name of the corresponding interface (e.g. *Local Area Connection*). You can get it either with the command *ipconfig /all* or through *Start -> Settings -> Control Panel -> Network and Dial-Up Connections*.

Use the following command to assign a static MAC address to the IP address of the default gateway:

> **netsh interface ipv4 set neighbors [interface=]<interface name> [address=]<IP> [neighbor]=<MAC> [store=]active**

Example:
netsh interface ipv4 set neighbors interface=LAN address=192.168.1.254 neighbor=00-aa-aa-aa-aa-aa store=active

You can verify the static assignment either with **arp –a** or with the command **netsh interface ipv4 show neighbors <interface name>**.

Use the following command to delete a static assigned MAC address:

> **netsh interface ipv4 delete neighbors [[name=]<Interface-Name>] [[address=]<IP>]**

Example:
netsh interface ipv4 delete neighbors LAN 192.168.1.254

Note: The static entry will be valid until the next reboot or until the next restart of the network connection due to the argument **store=active**. If you do not specify this argument the default value is **store=persistent**. In this case, the static entry will still exist after a reboot of the client even if you have deleted this entry with *netsh* and the argument **delete**. The only option you will have for getting rid of this static entry is to call **netsh interface ipv4 reset** and to restart the network connection.

2.3   Router Modes (Router, PPPoE/PPTP)

2.3.1   It is not possible to "ping" the mGuards external IP address

By default, the mGuard drops ICMP packets from the external network directed to its external interface. You can enable this option through the menu *Network Security -> Packet Filter*, tab *Advanced*, option *ICMP via primary external interface for the mGuard*.

2.3.2   When do I need to configure additional internal/external routes?

You need to define for example an additional internal route if the internal network contains a subnet which can be accessed through another router. In this case you need to specify as *Network* the network IP of the subnet and as *Gateway* the external IP address of the router.

Note: Do never specify an additional internal route for a network/gateway, which belongs to the external network and vice versa. This could cause a strange behaviour of the firewall.

2.3.3   I can't access the mGuard from the web browser

- Verify that the internal IP of the mGuard is defined as default gateway on the client.
- Did you use the correct IP address for accessing the mGuard? If the internal IP address of the mGuard is unknown execute the *Recovery* procedure (please refer to the *mGuard User Manual*). This procedure will reset the mGuard back to *Stealth* mode (except *mGuard delta*, *mGuard centerport* and *mGuard blade control unit*) so that you can access it through https://1.1.1.1. *mGuard delta*, *mGuard centerport* and *mGuard blade control unit* are reset to *Router* mode with the internal IP 192.168.1.1.
- Starting with version 3.1.0 it is possible to block SSH and HTTPS access from the internal network (HTTPS: menu *Management -> Web Settings*, tab *Access*, SSH: menu: *Management -> System Settings*, tab *Shell Access*). If you have specified such rules you need to execute the *Recovery* procedure. This procedure will remove SSH access rules and enable internal HTTPS access.

2.3.4   PPPoE mode: I can't access the Internet

- Verify that NAT (*Network Address Translation*) is enabled (menu *Network Security -> NAT*, tab *Masquerading*).
- If you can ping the IP address 212.21.76.70 but if you can't reach the site by its name (www.innominate.com) then you need to specify a name server in the network settings of your computer.

2.4   mGuard PCI

2.4.1   Why is the Rescue Switch not reachable from outside?

A hardware reset is not required because the mGuard PCI has a hardware watchdog. The watchdog tests every second if the Linux kernel is still alive. If the kernel should die for some strange reason then a reset is performed automatically and the kernel is restarted. A *Rescue Switch* located at the outside wouldn't provide more functionality than the watchdog. The advantage is that no one needs to go to the server room if the kernel dies. You can also initiate other additional functions with the *Rescue Switch* like for example the *Recovery* procedure which resets the mGuard to *Stealth* mode. This is another reason why the *Rescue Switch* shouldn't be accessible from outside to prevent misuse.

2.4.2   Is the mGuard PCI operable with PCI-x and PCI express slots?

PCI-x: This works if the mGuard PCI is operated in *Power-over-PCI* mode which means, that only the power is taken from the PCI slot.
PCI express: No.

3   Software Update, Recovery- and Flash Procedure

3.1   Software Update

3.1.1   Does the mGuard lose its configuration when performing a software update?

The mGuard won't lose its configuration when updating the firmware through the web interface. The configuration will be erased and reset to the default factory settings only when flashing the mGuard.

3.1.2   Offline update error message "tar: Invalid gzip magic"

Verify that the file extension of the update file you have downloaded is *.tar.gz (e.g. update-6.1.x-7.0.0.tar.gz). Sometimes Microsoft Internet Explorer saves the file as *.tar.tar when downloading it from our homepage which is an invalid format for the mGuard.

3.1.3   Online update error message "Not a valid hostname or IP address"

This error message usually occurs if the mGuard can't resolve the IP address of the update server *update.innominate.com*. Go to the menu *Network -> DNS*, set *Servers to query* to *User defined* and enter into the field *User defined name servers* the IP address of a valid DNS server.

If the mGuard is operated in *Stealth* mode, check if a desktop firewall is running on the client to which the mGuard is connected. If this is the case, the firewall must allow incoming ICMP requests. The mGuard in *Stealth* mode can't issue ARP requests by itself. Therefore it sends a specially marked ICMP echo request to the client and obtains the MAC address of the default gateway from the reply.

3.1.4   Online update error message "server returned error 404: HTTP/1.0 404 Not Found"

Starting with updates to version 3.0.0 the HTTPS protocol needs to be used. Go to the menu *Management -> Update*, tab *Update*, and verify that *Protocol* is set to *https://*.

3.1.5   Online update error message "HTTP/1.0 401 Authorization Required"

You need to provide your login parameters (user/password) for being able to download updates or the firmware from our update server. You'll receive this information after registering through our homepage (www.innominate.com *-> Services -> Software Updates*).
When configuring the update server (menu *Management -> Update*, tab *Update*) you also need to enter your username and password for accessing the download area. If one of those parameters is wrong or if those parameters are completely missing, the error message "HTTP/1.0 401 Authorization Required" is displayed. Username and password are case sensitive. You need to enter them as stated in our response mail to your online registration.

3.1.6   Update message "35 packages not installed completely"

The update process checks at first which packages are currently installed on the device and their version. Based on this information the update process determines which and how many packages need to be updated. The total numbers of packages which need to be updated are displayed in the message "xx packages not installed completely".

3.1.7   Update message "1 package not installed completely – Please reboot"

This is not an error message. The installation of the related package will be finished after rebooting the device.

3.2 Recovery Procedure

3.2.1 When do I need to execute the Recovery procedure?

You need to execute the *Recovery* procedure if you can't get access to the mGuard for one of the following reasons:

- The mGuard is operated in *Router*, *PPPoE* or *PPTP* mode and its internal IP is unknown. The *Recovery* procedure will reset the **mGuard delta**, **mGuard centerport** and **mGuard blade control unit** into *Router* mode and its internal IP to 192.168.1.1 so that the device is accessible again through https://192.168.1.1. All other products (**mGuard smart**, **mGuard industrial RS**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth* mode so that they are accessible again through https://1.1.1.1.
- The mGuard is operated in *Multiple Client Stealth* mode with a configured *Management IP* and this IP is unknown. The *Recovery* procedure will remove the *Management IP* so that the mGuard can be accessed again from the internal network through https://1.1.1.1.
- SSH and HTTPS access have been disabled for the internal interface and the remote access wasn't enabled for the external network. This feature is available starting with 3.1.0. The *Recovery* procedure will remove SSH access rules and enable internal HTTPS access.

3.2.2 Does the mGuard lose its configuration when executing the Recovery procedure?

The *Recovery* procedure won't affect current configured VPN connections, firewall settings or passwords, except the changes mentioned in the previous chapter.

3.3 Flash Procedure

3.3.1 When do I need to flash the mGuard?

You only need to flash the firmware of the mGuard if the root password is unknown. **Note that this procedure will erase existing configurations on the mGuard**. The mGuard will be restored to the factory (default) settings, also the passwords. You need to reconfigure the mGuard after flashing the firmware.

Note: If you want to update the version of the firmware then the *Update* procedure should be the preferred method.

3.3.2 How do I flash the mGuard?

Please download the document *mGuard Update-/Recovery-/Flash-Procedure* from our homepage (www.innominate.com *-> Downloads -> Documentation*). It describes in detail the required steps for flashing the mGuard.

3.3.3 Problems with Windows TFTP/DHCP server

The following steps are required if the IP address of the client has been changed since the last time you've started the TFTP server:
- Start the TFTP server and ignore appearing error messages.
- Click *<Settings>* and then *<OK>*.
- Restart the TFTP server.

3.3.4 mGuard smart: The middle LED flashes red after the DHCP server has sent the IP address

- Verify that the firmware files *image.p7s* and *jffs2.img.p7s* are located in the specified TFTP directory.
- On Linux: Check the access rights of the directory which contains the image files.

3.3.5 Error message "The system cannot find the file specified (rollout.sh)"

The file rollout.sh is only required, if the mGuard should be configured through a configuration file during the flash procedure. Otherwise this message can be ignored.

3.3.6 Error message "The system cannot find the file specified (licence.lic)"

It is possible to upload a license file to the mGuard during the flash procedure. The license file must be stored in the same directory which contains the firmware image files, either as *licence.lic* or as *<serial number>.lic*. You can ignore this message if no license file should be uploaded.

3.3.7 How do I configure the script rollout.sh?

Please download the application note *mGuard Rollout Support* from our homepage (www.innominate.com *-> Downloads ->Application Notes*). This document describes in detail the required steps for configuring the script rollout.sh.

Note: The script *rollout.sh* must be stored in UNIX format.

3.3.8 One LED displays S-O-S after flashing and rebooting the device

Starting with mGuard version 5 updating to the next major release (e.g. from 4.x.x to 5.x.x) requires a *Major Release Update* license (please refer to the document *mGuard Update-/Recovery-/Flash-Procedure* which can be downloaded from our homepage). Otherwise one LED displays S-O-S after flashing and rebooting the device. The *Major Release Update* license must be located in the same directory as the firmware image files and must have either the filename *licence.lic* or *<serial number>.lic*. The flash process looks automatically for those files being available.

3.3.9 TFTP server reports "rcvd packet too short"

This problem was caused by a defective hub. Replacing the hub by a switch solved the problem.

4   VPN

4.1   General Questions

4.1.1   License for 10 VPN tunnels: Does it mean a maximum of 10 VPN tunnels or 10 IP connections?

This license limits the maximum number of VPN tunnels that can be active on the mGuard, not the number of IP connections within a tunnel or the number of configured VPN connections.

4.1.2   In which cases can I use pre-shared secret keys (PSK) as authentication method?

You can use pre-shared secret keys (PSK), if:
- Both peers have a static IP address. Alternatively a peer with a dynamic public IP address can register its IP under a fixed name in a DynDNS service and the remote peer must refer to it.
- The VPN connection won't be established across one or more gateways that have *Network Address Translation* (NAT) activated.

In any other case certificates need to be used.

4.1.3   How do I obtain X.509 certificates?

The enrolment of certificates requires a certification authority (CA) which issues public key certificates for a specific period of time. A CA can be a private (in-house) CA, run by your own organization, or a public CA. A public CA is operated by a third party that you trust to validate the identity of each client or server to which it issues a certificate.

There are several tools available for creating and managing certificates, as for example Microsoft CA Server, OpenSSL and XCA. Please refer to the document *How to obtain X.509 Certificates* which can be downloaded from our homepage (www.innominate.com *-> Downloads -> Application Notes*).

4.1.4   How does Dead Peer Detection (DPD) work?

There are two parameters for configuring *Dead Peer Detection*: Delay and Timeout. The default settings are Delay=30 and Timeout=120. The mGuard will send *DPD Keep Alive* messages every 30 seconds through the ISAKMP SA to check the availability of the remote peer. If the remote peer does not answer within 120 seconds the mGuard will declare the peer as dead and execute the following action depending on the specified *Connection startup*:
- *Connection startup = Initiate*: The mGuard will try to re-establish the VPN tunnel.
- *Connection startup = Initiate on demand*: The VPN connection is put into trap and will be re-initiated the next time when traffic needs to be sent through the tunnel.
- *Connection startup = Wait*: The mGuard will delete the VPN connection and wait for the remote site to re-establish it.

👉 **Note:** DPD only works if both peers support it!

4.1.5   Does the remote peer support Dead Peer Detection (DPD)?

Please consult the user manual of the device or ask the manufacturer. Apart from this you can get this information also from the VPN logs (menu *Logging -> Browse local logs*, option *IPsec VPN* enabled). If you see there the message *Dead Peer Detection (RFC3706) enabled* before the IPsec SA is established, then the remote peer supports DPD.

4.1.6 What do I need to consider if both mGuards are located behind NAT gateways?

- Only one mGuard can initiate the connection. The other mGuard must wait for the connection. Do not configure both mGuards to initiate the connection.
- You must use X.509 certificates as authentication method. Pre shared keys (PSK) can only be used, if both peers have a static public IP address AND if the connection won't be established across one or more gateways that have Network Address Translation (NAT) activated.
- You need to enter %any as *Address of the remote site's VPN gateway* on the mGuard that waits for the connection.
- On the receiving site you need to define port forwarding on the NAT gateway for UDP port 500 and UDP port 4500 to the external IP address of the mGuard.

4.1.7 When do I need to use VPN 1:1 NAT for the local network?

VPN 1-to-1 NAT for the local network is used for establishing VPN tunnels to other locations which use the same network or to establish a VPN tunnel between two sites which use the same internal network. Please refer to the *mGuard Configuration Examples* which can be downloaded from our homepage (www.innominate.com -> *Downloads -> Documentation*).

4.1.8 Error message "Referenced entry is missing" after deleting a machine certificate

This message appears when trying to delete a machine certificate which is still referenced in a VPN connection. You can either edit the corresponding VPN connection, switch to the tab *Authentication* and set *Local X.509 Certificate* to *None* before deleting the machine certificate or import the new machine certificate first, edit the corresponding VPN connection, switch to the tab *Authentication*, select the new machine certificate as *Local X.509 Certificate* and delete then the old machine certificate.

4.2 VPN tunnel problems

4.2.1 VPN tunnel referring to a DynDNS name can't be established or fails after a while

Check if the service DynDNS monitoring (menu *IPsec VPN -> Global*, tab *DynDNS Monitoring*) is enabled. If it isn't enabled, the mGuard won't notice when the IP address of the remote gateway has changed.

4.2.2 VPN tunnel using DynDNS gets interrupted after a couple of hours

If you have specified a DynDNS name as address of the remote VPN gateway, ensure that DynDNS monitoring (menu *IPsec VPN -> Global*, tab *DynDNS Monitoring*) is enabled. Otherwise the mGuard won't notice when the IP address of the remote VPN gateway has changed.

4.2.3 PPPoE mode: Problems transferring huge data (e.g. database, email) through a VPN tunnel

The packages which reach the mGuard are already fragmented due to the Ethernet adapter to which the mGuard is connected. The Ethernet adapter (MTU=1500) fragments the packages and forwards them to the mGuard. Due to the encoding of the packages their size will increase slightly. This could cause problems at some ISP router if they don't support UDP fragmentation. You can reduce the MTU size for the VPN connection through the menu *IPsec VPN -> Global* if you encounter such a problem.

Another possibility is to reduce the MTU size of the Ethernet adapter of the sending entity.

4.2.4   VPN tunnel works in one direction only

- Ensure that the internal IP address of the mGuard is specified as default gateway on the clients of the internal network.
- Check if possibly configured VPN firewall rules may block the traffic in one direction or if on the target client a desktop firewall rejects the access.

4.2.5   A VPN tunnel can't be established. What could be the reason?

A VPN tunnel is established in two phases: Phase 1 (ISAKMP SA) and Phase 2 (IPsec SA).

Phase 1 (ISAKMP SA) couldn't be established:
- Mismatched Pre-shared secret keys (PSK) or certificates.
- Mismatched ISAKMP policy parameters (encryption/hash algorithm). Compare the *ISAKMP SA (Key exchange)* settings with the settings on the remote gateway.

Phase 1 (ISAKMP SA) could be established but not phase 2 (IPsec SA):
- Mismatched IPsec policy parameters (encryption/hash algorithm). Compare the *IPsec SA (Data exchange)* settings with the settings on the remote gateway.
- Mismatched tunnel settings:
    o The local and the remote network of the tunnel settings may not be within the same network IP. The following settings won't work: local network=192.168.1.0/16, remote network= 192.168.2.0/16. In this case the netmask must be changed to a C-Class (/24) netmask.
    o The local network of the mGuard must be specified as *remote network* on the remote gateway. The local network of the remote gateway must be specified as *remote network* on the mGuard.

4.2.6   VPN connection can't be established, the ipsec deamon isn't started

Is the option *Disable VPN until the user is authenticated via HTTP* (menu *Authentication -> Local Users*, tab *Passwords*) enabled? This option especially protects mGuards used by *Road Warrior* against unauthorized usage. The VPN connection won't be established as long as you did not enter the user password. The login screen appears as soon as you try to access any web page.

4.2.7   IPsec status: The displayed lifetimes differ from the settings

This is caused by the settings of *Rekeymargin* and *Rekeyfuzz*. If you set both to 0 then the displayed lifetimes would correspond to the settings of the ISAKMP SA and IPsec SA lifetimes. *Rekeymargin* specifies how long before SA (and key) expiry the mGuard should attempt to negotiate replacements. *Rekeyfuzz* specifies the maximum percentage by which *Rekeymargin* should be randomly increased to randomize rekeying intervals (important for hosts with many VPN connections). Both values are taken into account when the lifetimes are calculated which are displayed in the menu *IPsec VPN -> IPsec status*.

4.2.8 Stealth mode: Pluto restarts continuously (displayed in the VPN log)

VPN Log entries:
adding interface ipsec0/br0 10.196.148.183
adding interface ipsec0/br0 10.196.148.183:4500
…
shutting down interface ipsec0/br0 10.196.148.183
shutting down interface ipsec0/br0 10.196.148.183
…
listening for IKE messages
adding interface ipsec0/br0 192.168.110.1
adding interface ipsec0/br0 192.168.110.1:4500

Take a look at the VPN Log and check if always the same IP address is displayed for the ipsec0/br0 interfaces. If this is not the case, as shown in the example above, the problem can be caused by one of the following reasons:
• The mGuard is connected the wrong way round (LAN to WAN and WAN to LAN).
• The mGuard is operated in *Stealth autodetect* mode but multiple clients are connected to the internal interface.
• The mGuard is operated in *Stealth autodetect* mode and the NIC of the system, which is connected to the internal interface of the mGuard, has more than one IP address. This could be the case when using for example VMWARE.

Explanation: The mGuard (*Stealth autodetect* mode) gets its IP address by analyzing the traffic which comes from the internal network. When the IP address of the client has changed then the dependent services (e.g. pluto) will be restarted. During the restart of the services you will lose the connection to the external network and you also won't have access to the web interface. In *Stealth autodetect* mode only one client with only one IP address should be connected to the internal interface.

4.2.9 Poor VPN throughput in a Windows environment

Please read the application note *Windows 2000/XP TCP Tuning for High Bandwidth Networks* which can be downloaded from our homepage (www.innominate.com *-> Downloads -> Application Notes*).

Microsoft has really done a remarkable job. The TCP implementation includes virtually all of the recent extensions to improve performance but the default values of some parameters are too conservative and need to be adjusted for getting the optimum of performance. Usually you won't notice the reduced performance during your normal work but it gets visible when making performance measurement.

Tuning the Windows TCP settings according to this document will not only increase the VPN throughput. It will also increase the overall performance of your network.
For low delay networks we were able to increase the overall performance by a factor of **1.8** and the VPN throughput by a factor of **1.5**. For high delay networks with an RTT of 40ms we were able to increase the overall performance by a factor of **11.7** and the VPN throughput by a factor of **3.4**. This is a remarkable result, which makes it worth to tune the Windows TCP settings.

4.3 L2TP/IPsec

4.3.1 How do I setup an L2TP connection between a Windows client and the mGuard?

Please download the document *mGuard Configuration examples* from our homepage (www.innominate.com *-> Downloads -> Documentation*). It describes in detail the required steps for setting up an L2TP/IPsec connection between a Windows client and the mGuard.

Note: Using an L2TP/IPsec connection from a Windows client to the mGuard is not possible if the connection is NATed. In other words, this kind of connection can only be used if the Windows client and the mGuard are connected directly to the Internet. Otherwise a software VPN client, compliant to the IPsec standard, must be used on the Windows client for establishing the VPN connection to the mGuard.

4.3.2 Windows client error #789

- Verify that the Windows service *IPsec Policy Agent* is up and running. If you have installed a VPN client previously (e.g. SSH Sentinel) it is possible that this VPN client turned off this service.
- The L2TP server is not enabled on the mGuard (menu *IPsec VPN -> L2TP over IPsec*).
- The certificate is missing or something is wrong with the certificate on the Windows client. Start *MMC* on the Windows client and check the *Personal* certificate in *Console Root -> Certificates (Local computer)*.

4.3.3 Windows client error #792

- mGuard Log message: initial Main Mode message received on xxx.xxx.xxx.xxx:500 but no connection has been authorized with policy=RSASIG
- ⇒ Check which Windows Service Pack is installed and the selected encryption algorithm for the ISAKMP SA. W2k without SP supports only DES, starting with SP2 3DES is also supported.

4.4 Interoperability

4.4.1 How do I setup a VPN tunnel between the mGuard and an appliance from another vendor?

Please check the download section of our homepage (www.innominate.com -> *Downloads -> Application Notes*). There you'll find several interoperability guides which explain in detail how to setup a VPN tunnel between the mGuard and one of the following appliances:
* Astaro V5/V6
* Astaro Security Gateway 220
* Bintec VPN Access 25
* Check Point NGX (R60)
* Cisco 1812
* Cisco ASA
* Cisco PIX
* Cisco VPN3000 Concentrator
* Fortigate 60
* Microsoft ISA Server 2004
* NETGEAR FVS338
* Netscreen 5GT/204/5400
* TrustGate5

4.4.2 VPN problems with Cisco devices

Usually the ISAKMP SA and IPsec SA lifetimes are negotiated when the connection is established, even if different values are specified on the gateways. Cisco devices require that exactly the same values for the ISAKMP SA and IPsec SA lifetimes are defined on both gateways. Verify this when encountering problems with a VPN connection between the mGuard and a Cisco device.

4.4.3 Problems establishing a VPN across a Lancom router (model 1611)

This problem may occur when using an older firmware version (e.g. 3.5x) of the router. Upgrade the router to a current firmware version (e.g. 5.x).

4.4.4 Problems establishing a VPN across a T-Sinus (T-Com) router

General port forwarding doesn't work on the T-Sinus router. Port forwarding only works for registered participants.

4.4.5 VPN tunnel between mGuard and Astaro doesn't work

* When using X.509 certificates, ensure that *X.509v3 Distinguished Name (DN)* is selected as VPN identifier on the Astaro.
* Ensure that *IP Compression* is turned off on the Astaro. The mGuard does not support this feature.

5   Firewall

5.1   Which rules do I need to follow when configuring the firewall?

▪ The firewall rules will be checked one by one, starting with the first rule. If one rule matches the criteria, independent from the action (Accept, Reject or Drop), then the following rules won't be considered.
▪ The entries *From Port* and *To Port* are only considered if *Protocol* is set to UDP or TCP. Otherwise those entries won't have any effect. Note that the following rule will reject all data packets because of Protocol=All and therefore the specified *To Port=80* will be ignored: Protocol=All, From IP=0.0.0.0/0, From Port=any, To IP=0.0.0.0/0, To Port=80, Action=Reject

5.2   Do I also need to configure incoming firewall rules?

You only need to do this if you'd like to make services of the internal network accessible for other users of the external network. The mGuard uses *stateful filtering*. If a connection to the external network was established from a computer of the internal network, the firewall will let in all data packets which belong to this connection.

5.3   I'd like to prevent access to the Internet but it doesn't work

• You need to specify *Protocol=TCP*, *From Port=any*, *To Port=80* and *Action=Drop/Reject* for preventing access to the Internet. If you also have specified *From Port=80* this rule will never match because HTTP requests from web browser use a port >= 1024.

5.4   What's the meaning of the abbreviations in the firewall log?

Please refer to the application note *mGuard Firewall Logging* which can be downloaded from our homepage (www.innominate.com *-> Downloads -> Application Notes*).

5.5   ICMP echo requests from the client to the mGuard do not appear in the FW log

This is correct because those ICMP packets do not need to pass the firewall.

5.6   I can reach the clients of the internal network through port forwarding although the incoming firewall should prevent it

This is correct. Port forwarding has a higher priority than the firewall, therefore port forwarding overrules the incoming firewall.

5.7   MAC filter: Restricted IPv4 access doesn't work

The IPv4 access to the internal network of the mGuard should be restricted for a subset of MAC addresses. Nevertheless it is possible to gain access to the internal network from any other machine of the external network. In contrast to the stateful inspection firewall, all ARP and IPv4 frames will pass the MAC filter by default. If the MAC filter should restrict the access for specific MAC addresses then you need to define a final rule for IPv4, which drops everything else.
        Source MAC = xx:xx:xx:xx:xx:xx
        Destination MAC = xx:xx:xx:xx:xx:xx
        Ethernet protocol = IPv4
        Action = Drop

Note: MAC filtering is only supported for the *Stealth* mode.

5.8   When do I need to use 1:1 NAT?

1:1 NAT is used for example for connecting several subnets with the same network IP (e.g. 192.168.1.0/24) to the "main" network. 1:1 NAT mirrors addresses from the internal network to the external network. Depending on the specified subnet mask the host address field of the IP address will be kept unchanged and the network address is masqueraded. Please refer to the *mGuard Configuration Examples* which can be downloaded from our homepage (www.innominate.com *-> Downloads -> Documentation*).

5.9   Poor firewall throughput

Go to the menu *Network -> Interfaces*, tab *Ethernet* and check the current transfer mode (FDX = Full Duplex, HDX = Half Duplex) of the interfaces. It is possible that one of the interfaces uses HDX even if the network uses FDX. This can be caused by some NICs in the network which are not configured to use auto-negotiation or do not support auto-negotiation correctly. In those cases the mGuard can detect the transfer rate but not the transfer mode and will switch to HDX. This of course will reduce the performance.

If one of the interfaces use HDX and you are sure that the network uses FDX, set *Automatic Configuration = No* and specify the desired transfer rate and transfer mode with the *Manual Configuration* settings.

6   User Firewall

6.1   The remote user has been logged out but he still can use the connection

This behaviour is correct. If a remote user has been logged out he can't establish new connections but he still can use existing connections as long as they persist in the connection tracking table.

Protocol	Lifetime of unused connections
TCP	5 days
UDP	30s (unidirectional traffic) 180s (bidirectional traffic)
ICMP	30s
Others	10min

Unused TCP connections will be deleted after 5 days (default value) from the connection tracking table. This value can be changed through the menu *Network Security -> Packet Filter*, tab *Advanced*.

7   Services

7.1   I have entered a NTP server and enabled this service but it doesn't work

You also need to specify a valid name server (menu *Network -> DNS*, tab *DNS Server*). Otherwise the IP address of the NTP server can't be resolved.

7.2   Problems with DHCP Relay

Consider the following points when configuring DHCP relay:
- The mGuard must have a static external IP address.
- The DHCP server must know to which gateway the response needs to be sent. On the DHCP server, you must either specify the external IP address of the mGuard as default gateway or add a route to the internal network of the mGuard.

7.3   How do I need to configure the mGuard for using DynDNS.org?

In the following example we want to configure the mGuard to register its public IP address under the name *mguard.dyndns.org*:

Menu: *Network -> DNS*, tab *DynDNS*

Registration Register this mGuard at a DynDNS Service? = Yes
Refresh Interval (sec) = 3600
DynDNS Provider = DynDNS.org
DynDNS Server = dyndns
DynDNS Login = <username>
DynDNS Passwort = <password>
DynDNS Hostname = mguard.dyndns.org

8   Third Party Products

8.1   Stealth mode: Cisco firmware upgrade through TFTP doesn't work

Even if the TFTP server is started on the client, the upload will be initiated by the Cisco router. Therefore the incoming firewall of the mGuard must allow UDP traffic on port 69.

8.2   Stealth mode: Access to Lotus Notes server with mGuard 10-20 times slower

Go to the menu *Network -> Interfaces*, tab *Ethernet*, and check the current transfer mode (FDX = Full Duplex, HDX = Half Duplex) of the interfaces. It is possible that one of the interfaces uses HDX even if the network uses FDX. This can be caused by some NICs in the network which are not configured to use auto-negotiation or does not support auto-negotiation correctly. In those cases the mGuard can detect the transfer rate but not the transfer mode and will switch to HDX. This of course will reduce the performance.

If one of the interfaces use HDX and you are sure that the network uses FDX, set *Automatic Configuration = No* and specify the desired transfer rate and transfer mode with the *Manual Configuration* settings.

8.3   Does the mGuard support Novell IPX?

The mGuard does not support IP/IPX because this is a non routable protocol. The mGuard supports MAC filtering starting with version 3.0.0. With this feature it is possible to allow IPX frames to pass in both directions. If rules are specified for other Ethernet protocols than IPv4 and ARP, no filtering will take place except for the MAC address. Note that MAC filtering is supported for *Stealth* mode only.

8.4   Stealth mode: Problems with Microsoft Server and Network Load Balancing (NLB)

The following needs to be considered if you want to secure Microsoft servers, which form a cluster using *Network Load Balancing* (NLB), with mGuards (*Stealth* mode):

The Microsoft servers exchange information using a proprietary Ethernet protocol with the hex value 886f. Usually the mGuard will block this protocol. The mGuard supports MAC filtering starting with version 3.0.0. With this feature it is possible to allow this protocol to pass the mGuard in both directions.
Apart from this the mGuard needs to be operated in *multiple client stealth* mode because the NICs of the servers have more than one IP address.

Menu *Network Security-> Packet Filter*, tab *MAC Filtering*: The MAC filter is stateless in contrast to the IPv4 stateful inspection firewall. This means that rules must be defined for both directions. You need to define an incoming and outgoing rule with the following parameters for allowing the NLB protocol to pass:

> Source MAC = xx:xx:xx:xx:xx:xx
> Destination MAC = xx:xx:xx:xx:xx:xx
> Ethernet Protocol = 886f
> Action = Accept

Note that no filtering except for the MAC address will take place if other protocols are used than IPv4 and ARP.

9 Related Documentation

The following documents can be downloaded from our homepage (www.innominate.com -> *Downloads -> Documentation* and *Downloads -> Application Notes*). Please check our homepage periodically for updated or additional documents.

User Manual
• mGuard User Manual

Application Notes
• Windows 2000/XP TCP Tuning for High Bandwidth Networks
• Innominate mGuard Rollout Support
• How to obtain X.509 Certificates
• Firewall Logging

Additional Documentation
• mGuard Configuration Examples
• mGuard Update-/Recovery-/Flash-Procedures

Interoperability Guides
How to setup a VPN tunnel between the mGuard and one of the following devices:
• Astaro V5/V6 (PSK and X.509 Certificates)
• Astaro Security Gateway 220 (PSK and X.509 Certificates)
• Bintec VPN Access 25 (PSK and X.509 Certificates)
• Check Point NGX (R60) (PSK and X.509 Certificates)
• Cisco 1812 (PSK and X.509 Certificates)
• Cisco ASA (PSK and X.509 Certificates)
• Cisco PIX (PSK and X.509 Certificates)
• Cisco VPN3000 Concentrator (PSK and X.509 Certificates)
• Fortigate 60 (PSK and X.509 Certificates)
• Microsoft ISA Server 2004 (PSK and X.509 Certificates)
• NETGEAR FVS338 (PSK and X.509 Certificates)
• Netscreen 5GT/204/5400 (PSK and X.509 Certificates)
• TrustGate5 (PSK and X.509 Certificates)